Government cuts cyber-attack fix times by 84% and launches new profession to protect public services

26.2.2026 - | Her Majesty's Revenue and Customs

The government has launched a new vulnerability monitoring service (VMS) to reduce cyber risks and speed up fixes, and a new Cyber Profession to build long-term resilience across public services.

- Critical cyber weaknesses across the public sector will now be fixed 6 times faster than before.
- Ministers are determined to go further — with first-ever dedicated government Cyber Profession to give the state the skilled staff it needs to protect UK's key services from cyber threats.
- The number of serious unresolved cyber security weaknesses across government cut by three quarters as part of government-wide efforts to strengthen Britain's digital defences.

Public services millions of people depend on – from the NHS to the Legal Aid Agency – are becoming significantly safer and more resilient thanks to major improvements by the government to identify and fix cyber threats.

A specialist government monitoring service, introduced as part of the Blueprint for modern digital government, published in January 2025, means serious security weaknesses in public sector websites are fixed 6 times faster – cutting the average time from nearly 2 months to just over a week.

The vulnerabilities are in the Domain Name System (DNS) — the internet's address book that turns website names into the numbers computers use to find them. Weaknesses in DNS can allow attackers to redirect users to fraudulent sites, steal sensitive data, or take services offline entirely — with potentially serious consequences for anyone relying on government services.

Before this service was in place, a weakness in a government DNS record could go unnoticed for nearly 2 months — long enough for a hostile actor to redirect someone trying to access a government service to a fake site designed to steal their personal details, intercept sensitive communications, or disrupt services that people rely on. The vulnerability monitoring service has closed this window down to 8 days. It alerts the right people with clear, practical guidance on how to fix the problem, and tracks progress until each issue is resolved.

Speaking at the annual Government Cyber Security and Digital Resilience conference, Digital Government Minister Ian Murray will outline how this will sharply reduce the risk of hackers targeting essential services like the NHS.

He'll also outline how the government has reduced its backlog of these vulnerabilities by 75% — significantly shrinking the window for cyber criminals to target essential public services – from GP surgeries and ambulance trusts to hospitals and social care providers.

Today's announcement marks a decisive step in closing the door on such threats with the government going even further with the launch of the first-ever dedicated government Cyber

Profession. This programme will recruit and train the top-tier cyber experts needed to keep public services safe.

Minister for Digital Government Ian Murray said:

> Cyber-attacks aren't abstract threats — they delay NHS appointments, disrupt essential services, and put people's most sensitive data at risk. When public services struggle it's families, patients and frontline workers that feel it.
>
> The vulnerability monitoring service has transformed how quickly we can spot and fix weaknesses before they're exploited so we can protect against that. We've cut cyber-attack fix times by 84% and reduced the backlog of critical issues by three quarters. And as the service expands to cover more types of cyber threats, fix times are falling there too.
>
> But technology alone isn't enough. Today I'm launching a new government Cyber Profession to attract and develop the talented people we need to stay ahead of increasingly sophisticated threats - making government a destination of choice for cyber professionals who want to protect the services that matter most to people's lives.

Dr Richard Horne, CEO of the NCSC, said:

> Cyber security is more consequential than ever today with attacks in the headlines showing the profound impacts they can have on people's everyday lives and livelihoods.
>
> As our public services continue to innovate, it is vital that they remain resilient to evolving threats and vulnerabilities are being effectively managed to reduce the chances of disruption.
>
> The government Cyber Action Plan is a crucial step in building stronger cyber defences across our public services and the launch of the government Cyber Profession today will help attract and retain the most talented professionals with the top-tier skills needed to keep the UK safe online.

The VMS continuously scans 6,000 UK public sector bodies, detecting around 1,000 different types of cyber vulnerabilities. When a weakness is identified, the service alerts the relevant organisation with specific, actionable guidance and tracks progress until the issue is resolved.

By automating detection and streamlining remediation, the service has:

- reduced median time to fix domain-related vulnerabilities from 50 days to 8 days — an 84% improvement
- reduced median time to fix other cyber vulnerabilities from 53 days to 32 days
- cut the backlog of critical open domain-related vulnerabilities by 75%
- processed and resolved around 400 confirmed vulnerabilities each month

The new government Cyber Profession is co-branded with the Department for Science, Innovation and Technology and the National Cyber Security Centre. It will introduce a competitive total employee offer, establish a dedicated Cyber Resourcing Hub to streamline recruitment, and create a clear career framework aligned with UK Cyber Security Council professional standards.

It will also include a government Cyber Academy for training and development, a new apprenticeship scheme to build future talent, and structured career pathways to strengthen long-term capability across the public sector.

The North West will serve as a primary hub for the profession, building on Manchester's growing digital ecosystem and the forthcoming government Digital Campus.

Notes to Editors:

The vulnerability monitoring service is a DSIT service that identifies domain and cyber vulnerabilities at scale across the public sector. It uses commercial and proprietary scanning tools to detect vulnerabilities in public sector internet-facing assets. The service detects vulnerabilities continuously – the remediation timeframes cited refer to the time taken for organisations to implement fixes once alerted.

The VMS was launched as part of the government's Blueprint for modern digital government, published in January 2025, which committed to a new cross-government vulnerability scanning service as one of 5 flagship kickstarter initiatives.

The £210 million investment forms part of the government Cyber Action Plan announced in the Minister's speech.

The NAO report Government cyber resilience (January 2025) found that the cyber threat to government is severe and advancing quickly, with skills gaps the biggest risk to building cyber resilience.

https://www.gov.uk/government/news/government-cuts-cyber-attack-fix-times-by-84-and-launches-new-profession-to-protect-public-services